Testimony of Michael A. Vatis
Director, Institute for Security Technology Studies at Dartmouth College
and
Chairman, Institute for Information Infrastructure Protection
Before the U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

April 8, 2003

Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection

Mr. Chairman, Madam Vice Chair, Ranking Member Clay, and Members of the Subcommittee. I would like to thank you for the opportunity to testify before you today on the subject of cybersecurity. This issue is one that has been with us as long as we have had computers. But it has grown in importance in recent years as both our economy and our national security become increasingly dependent on the security of computer and information networks. This is not only a problem for the future. It is a very real problem right now. And though we face many other challenges to both our economic and national security today, the problem of cybersecurity is unique in its complexity and in its rapidly evolving character. I therefore applaud this Subcommittee for recognizing the importance of this issue.

In the immediate aftermath of the terrorist attacks of September 11, 2001, commentators and government officials described America's inability to detect and prevent the terrorists' plot as a "failure of imagination." No one imagined, they claimed, that terrorists would be able to hijack four airliners simultaneously and then crash three of the four into significant economic and political landmarks. No one could have predicted, the early story went, that terrorists would deviate from the normal course of hijackings, in which hostages were taken and used as bargaining chips for some political goal or in which the objective was simply to blow up the plane in order to kill its passengers.

Soon it became apparent, however, that this explanation was far off the mark. In fact, the U.S. intelligence community had ample indications that terrorists might attempt to hijack planes and turn them into guided missiles. In 1994, for instance, Algerian terrorists hijacked an Air France plane with 227 passengers and crew on board, wired it with explosives, and loaded it with three times the fuel needed to fly from Algeria to France. Their intention: to use the plane as a bomb and crash it into the Eiffel Tower. This fact was well known to U.S. intelligence agencies. Those agencies also knew as early as 1995 that terrorists – including Ramzi Yousef, the mastermind of the first World Trade Center bombing – had planned to crash a private aircraft into the CIA Headquarters building in Langley, Virginia. And FBI agents knew for years that suspected terrorists were taking flying lessons in the United States. By August 2001, some agents and CIA officers had come to believe that some of these student pilots might be plotting airline suicide attacks.

Our Nation's vulnerability to such attacks was also apparent. It was clear for years before September 11 that weapons could easily be smuggled onto passenger planes, and that airplanes could be flown into sensitive airspace. Indeed, in 1994 a man crash-landed a stolen Cessna on the South Lawn of the White House grounds.

So, the events of September 11 were not unimaginable at all. The vulnerabilities were evident to anyone who paid attention, and the intentions of terrorists to commit acts similar to those that occurred on 9/11 had already been demonstrated. We just failed to take the necessary precautions – such as treating intelligence about suspected terrorists' flying lessons more seriously or adequately beefing up airport security to make smuggling a weapon on board a plane more difficult.

September 11 thus reminded us of a painful lesson: that we as a Nation – not just our law enforcement and intelligence agencies, but the entire Executive Branch, Congress, the news media, and the public – too often fail to treat new threats seriously and take the necessary steps to deal with them until after those threats have manifested themselves, often in catastrophic fashion. It has proven to be too difficult to muster the political will, avoid the distraction of more immediate concerns, and focus the attention of enough government officials or public opinion makers on such problems unless and until a major attack takes place and causes a significant loss of life or major economic disruption.

The Nation's response to the possibility of cyber attacks is in some ways an even more glaring example of this problem. For in the cyber arena, not only can we *imagine* serious cyber attacks based on the conjunction of our network vulnerabilities and the known intentions of would-be attackers, but we've actually *experienced* such attacks for over a decade. As long ago as the 1980s – ancient history in the Internet Age, when many of today's younger hackers were still in diapers – we saw the "Morris Worm" wreak havoc on the early Internet as it spread from computer to computer and caused victimized systems to cease functioning. We also saw the first known instance of cyber espionage, as West German hackers stole information from U.S. military networks and sold it to the Soviet KGB – an episode immortalized in Clifford Stohl's book, *The Cuckoo's Egg*. And throughout the 1990s and into the early 21st century, we have witnessed a steady escalation in the number and severity of attacks – ranging from politically motivated defacements or obstructions of government and private company websites; to Denial of Service Attacks against e-commerce and online news sites and Internet domain name root servers; to destructive worms and viruses that have caused significant harm to companies around the world; to intrusions by organized criminal groups into university and company networks for the sake of stealing proprietary information, credit card numbers, or money or to extort the system owner; and to intrusions into government networks to steal sensitive information. These attacks demonstrate not only that our information networks remain vulnerable to attack, but also that myriad bad actors are willing and able to exploit those vulnerabilities.

Moreover, publicly available information demonstrates that at least several foreign nation states have developed information warfare programs that could be used to target vital U.S. systems in the event of military conflict. Indeed, the Director of Central Intelligence has testified to this fact several times over the last five years. And news reports confirm what has long been feared – that al Qaeda has at least thought seriously about engaging in cyber attacks, and may have mapped out potential targets within America's critical infrastructures. Thus, while we have not yet – to our knowledge at least – experienced an actual instance of "cyber terrorism" or "information warfare" against the United States, if anything the indicators warning of the risk of such attacks vastly exceed the indicators that existed prior to September 11, 2001 of an aerial assault on the World Trade Center and Pentagon.

For many years, skeptics have pooh-poohed the cyber threat by saying that the only real threat comes from American teenagers joyriding on networks or engaging in the cyber equivalent of vandalism, or that the government has over-hyped the problem in order to invent new missions in the Post-Cold War world. But if kids can crash networks through denial of service or worm attacks or obtain system administrator level control of military or commercial networks, as we've seen on numerous occasions, surely it stands to reason that a sophisticated, and well funded, foreign military or intelligence organization or a terrorist group could accomplish the same – and much worse.

Of course, to say that cyber networks are vulnerable does not mean that the critical infrastructures that rely on those networks – such as electrical power grids, pipelines, telecommunications switching nodes, hospitals, etc. – are necessarily vulnerable, or that a cyber attack would have a sufficiently long-lasting, destructive impact to achieve a terrorist's or nation state's military or political objectives. We still do not actually know the full extent of our critical infrastructures' vulnerabilities to various types of cyber attacks and the extent of their potential impact. But it is clear at the least that computer networks themselves can be intruded into; that information can be stolen or altered in ways that could profoundly affect public confidence or the economy; that network functionality can be halted or degraded through denial of service attacks or the implantation of malicious code; and that reliant infrastructures can be impeded at least temporarily. The threat is real – we just don't yet understand the full scope of it, in part because of the complexity of infrastructures' reliance on networks and of the interdependencies among critical infrastructures. And we shouldn't wait for a major infrastructure attack to occur before we take steps to truly *learn* the full scope of our vulnerability, and to begin shoring up our weaknesses.

Yet, the willingness of both the government and the private sector to dedicate the attention and resources necessary to deal with the problem effectively has lagged. To its credit, the federal government did begin, in the mid 1990s, to take the cyber threat seriously and initiate efforts to address it. After commissioning both an internal group and a joint public-private commission to study the problem, the Clinton Administration issued Presidential Decision Directive (PDD) 63 in 1998, which set out the first federal policy framework and created new government and public-private structures to address our vulnerability to cyber attack. In 2000, the White House issued the National Plan for Information Systems Protection, the first comprehensive strategy to deal with this issue. The Bush Administration built on these efforts with the creation of the President's Critical Infrastructure Protection Board in 2001 and the issuance of a National Strategy to Secure Cyberspace in February 2003.

Despite the government's early grasp of the issue, however, its proposed solutions have not kept pace with the fast growth of the problem. Many of its initiatives have never received adequate funding to accomplish their assigned tasks. Government agencies' efforts to secure their own networks have consistently received failing marks from congressional watchdogs, including in the most recent report by the General Accounting Office. And funding for research and development of cybersecurity technologies has remained, in Representative Sherwood Boehlert's phrase, a "backwater."

After September 11, this situation appeared to be changing, apparently as a result of the vastly increased concern about *all* threats to our domestic security. Funding for some government cybersecurity activities has begun to increase. And research and development for cybersecurity appears to be poised for significant funding increases, perhaps by FY 2004, if actual appropriations match the authorization of funding increases in the Cyber Security Research and Development Act, which was signed into law last November.

But recent events seem to indicate that the government's efforts in this area are seriously regressing. First, with the dismantling of the President's Critical Infrastructure Protection Board (PCIPB) and the White House Office of Cyberspace Security, there is now a gaping void in the Executive Branch's leadership. There is no longer any central locus for cyber security policymaking, for implementation of government-wide initiatives, or for outreach to private industry. These functions are now supposed to be carried out mainly by the new Department of Homeland Security. But the positions responsible for these tasks – including the Undersecretary for Intelligence Analysis and Infrastructure Protection (IAIP), and the Assistant Secretaries for Intelligence Analysis (IA) and for Infrastructure Protection (IP), have not yet been formally nominated, let alone confirmed by the Senate. (In March, President Bush announced his intention to nominate Frank Libutti for the Undersecretary post, Paul Redmond for Assistant Secretary for IA, and Robert Liscouski for Assistant Secretary for IP, but has not actually nominated any of them yet.) The sooner these positions are filled, the quicker the DHS can begin aggressively addressing the cybersecurity part of its mission.

Even when these positions are filled, though, there will be no office responsible solely for cybersecurity policy and coordination. Rather, the Administration apparently intends to treat cybersecurity solely as a component of the broader "critical infrastructure problem," which includes vulnerability to physical terrorist attacks. Given the effort and attention being given to the risk of physical attack during the ongoing "war on terrorism," it seems quite likely that the lack of an office dedicated to cybersecurity will lead to that issue's getting short shrift. Rumors continue to float around Washington that Howard

Schmidt, the former Vice Chair of the PCIPB and a widely respected expert in the field, is being considered as a "special advisor" on cybersecurity to Secretary Tom Ridge. But no decision has yet been made, and even this position would apparently lack any "line authority" within the Department, and so would not adequately solve the problem.

These changes themselves suggest that the Administration has purposely reduced the level of priority it is devoting to cybersecurity policy – despite the expected protestations to the contrary. The uncharacteristically quiet manner in which the National Strategy to Secure Cyberspace was released (on Friday, February 14) – in contrast to the public trumpeting of the initial draft of the plan in September 2002 – seems to confirm this suspicion.

A second area of regression has to do with the loss of operational capability, particularly in the areas of detection, analysis, and warning of cyber threats. Last month, several government entities responsible for some aspect of cybersecurity were transferred to the new DHS, including: the parts of the National Infrastructure Protection Center responsible for analysis, warning, and outreach (the investigative arm of the NIPC remains at the Federal Bureau of Investigation); the Critical Infrastructure Assurance Office (CIAO); the National Communications System; the National Infrastructure Simulation and Analysis Center; the Energy Assurance Office; and the Federal Computer Incident Response Center (FedCIRC). On its face, this consolidation should improve the government's ability to gather, analyze and disseminate information regarding vulnerabilities, threats, and incidents, and to engage with private industry. And it may do so in time. But it appears that at least some of the consolidation involves less than meets the eye.

For example, with the transfer of most of the NIPC to DHS, over three hundred *positions* were moved from the FBI to DHS. Yet, because most of the actual *people* filling those positions found other jobs at the FBI after the DHS was first proposed, only about 10-20 personnel have actually made the move. Thus, for the most part, it is vacant "FTEs" (full-time equivalents) that have been transferred to DHS, not analysts ready to hit the ground running. What this means is that the DHS's capacity to collect information on cyber threats, analyze the information, and issue warnings is going to be seriously lacking – despite the valiant efforts of the people at DHS now – until hundreds of jobs are filled, senior leadership is in place, and the new structure of the IAIP directorate is worked out and responsibilities assigned. Given how long government hiring usually takes, especially with the necessity of background investigations, it could take a year, or considerably more, for the DHS even to get back to the level of functionality that the NIPC had achieved in its five years of existence. Given that the number and severity of cyber attacks continues to increase, this regression in our warning, analysis and response capability is troubling.

In another major respect, the government's efforts have not regressed, but also have not progressed sufficiently given the magnitude of the problem. When it comes to addressing the myriad vulnerabilities in the privately owned systems that constitute the bulk of the Information Infrastructure, the government continues to rely essentially on what I call the "soapbox strategy": warning of the urgency of the problem, urging hardware and software manufacturers to make more secure products, and cajoling owners and operators of critical business networks and utilities to devote more attention and resources to their own cybersecurity. Over the last five years, the government has consistently and vociferously rejected any talk of regulating vendors or users. And while it has not completely dismissed the notion of creating market incentives to enhance security, it has not encouraged such measures either.

The National Strategy to Secure Cyberspace continues in this vein. While it recognizes "vulnerability reduction" as part of one of its five priorities, the *means* it proposes to employ to achieve those reductions are essentially the same as those of the last Administration – urging "public private partnerships" to share information about threats and vulnerabilities and develop "best practices" for cybersecurity; and promoting research and development of more secure information systems. The strategy contains many good ideas. But I am afraid that without a more imaginative, and aggressive, set of strategies to implement them, they are likely to remain only ideas.

Good arguments can be, and have been, made against direct government intervention in this fast-moving, high-tech area. But it seems clear after more than five years that the "soapbox" strategy is not sufficient – and I say this as a veteran "soapboxer." Vulnerabilities in software persist. Attacks continue to increase. And the possibility of a significant attack by a sophisticated adversary – whether a nation state, a terrorist group, or a criminal group – remains, and in fact is growing as existing and potential future adversaries develop cyber attack capabilities. Clearly more is needed to secure our vulnerable systems. The question is what.

During the course of 2002, the Institute for Information Infrastructure Protection (I3P), a consortium of 23 leading academic and not-for-profit cybersecurity R&D organizations, hosted a series of workshops with software and hardware manufacturers, researchers, large corporate users, infrastructure owners and operators, and government officials to gather input for a national cybersecurity R&D agenda. During those workshops, which were focused largely on technical requirements and technology R&D priorities, it was striking how often experts from all of the communities stressed the need for changes in the legal, policy, and economic environment that affects cybersecurity. Without such changes, these experts asserted, advances in technical R&D would never suffice, because there would not be an adequate market for more secure products and for new security technologies.

Of course, a catastrophic cyber attack that affected numerous entities could quickly create such a market. But the goal should be to *avoid* such an attack, not wait for one to induce market forces. The question, then, is what measures can be taken to create or encourage a market for security – one that results in manufacturers making more secure products and owners of critical networks operating their networks more securely.

At the very least, research is needed to understand better the nature of the security market and the forces that affect it today and that are likely to affect it tomorrow as business transactions continue to migrate to the Internet. We must start with a clear assessment of the risks and economic costs that stem from cyber insecurity. Again and again during the I3P agenda development process, we heard that corporate executives and government officials lack a solid understanding of the true nature of the risk to their enterprises, including the potential costs of various types of attacks, and of the costs and benefits of varying levels of security that they could implement. Cost-benefit calculations are therefore extremely difficult and often forsaken altogether.

Beyond that, we need a better understanding of the potential levers that the federal and state governments could use to improve the state of security. This is, of course, where Congress can play a critical role. Direct regulation is of course one possibility. And indeed, like it or not, some regulation is already occurring, though in limited or indirect ways. In the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, for example, Congress imposed on health care providers and financial services firms, respectively, general requirements to take steps to ensure the security of their electronic systems. These measures were passed not out of a concern for security per se, but out of concern for protecting the privacy of patient and customer records stored on companies' networks. But the effect on the companies is the same as a regulation of security for security's sake. In addition, the Federal Trade Commission brought unfair trading practice actions against – and reached settlements with – Microsoft and Eli Lilly, claiming that both had misled consumers by not having in place security measures sufficient to live up to their promises about the security and privacy of customer information. Both settlements required the companies to institute security measures, and the FTC's actions can be viewed as setting de facto security standards for companies that handle consumer information. Finally, a new California law (effective July 1, 2003) requires entities conducting business in California to disclose computer security breaches if the breaches result in unauthorized access to California residents' unencrypted personal information (such as account, credit card, driver's license, or social security numbers). The law also provides for a civil damage action by injured customers against businesses that violate the new law. This law is likely to have broad national impact in light of the number of companies that "conduct business" in California. These varying approaches can be seen as experiments in regulation that might have broader applicability. At the very least, study is required to determine their efficacy in improving security, and their costs.

Consideration should also be given to "softer" approaches designed to foster greater security without stifling technical innovation. These might include tax incentives to increase network security expenditures; legislation to create or enhance liability on the part of manufacturers or network operators for negligent actions or omissions that harm others; insurance requirements or incentives for security investments; requirements for public companies to include a discussion of potential cyber risks or actual security breaches in their annual Form 10-K disclosure, in order to promote CEO and Board attention to security (similar to the approach utilized by the SEC to address Y2K concerns); and general standards or best practices for hardware and software manufacturers or certain critical industries. Rather than simply dismiss these types of approaches out of hand, we should acquire a solid understanding of their pros and cons and then pursue the best options.

Finally, the public discussion and understanding of the problem of cybersecurity would greatly benefit from more precision in terminology. For instance, "cyber terrorism" should not be used to describe run-of-the-mill web site defacements, network intrusions, or even denial of service attacks. That term at most should be reserved for truly destructive cyber attacks that cause death, injury, significant economic loss, or significant disruption of a critical infrastructure, and that are motivated by a desire to coerce or intimidate a government or civilian population in pursuit of some political, religious, or ideological end. To call even low-grade, routine attacks cyber terrorism risks losing credibility with company executives, government officials, and the general public – the very people from whom concerted action is needed. And we need to be careful to distinguish among the various forms of cyber attacks – whether they be cyber extortion, cyber vandalism, cyber theft, cyber espionage, cyber terrorism, or information warfare. Some of these already occur on a daily basis (like cyber theft and vandalism); some are undoubtedly occurring but are not known publicly, or perhaps even by our intelligence agencies (such as cyber espionage); and some have not yet occurred but are a distinct possibility (such as cyber terrorism and information warfare). And when we're not yet sure how to characterize an attack, we should simply refer to it as a "cyber attack" until sufficient information is available to understand the nature of the attack and the motivation of the attacker.

Conclusion

Cyber attacks are a real and growing threat. As the most information technology-dependent country in the world's history, we remain uniquely vulnerable to cyber attacks that could disrupt our economy or undermine our security. And yet our response as a society is still stuck in second gear. If we are to deal with this problem effectively, no options should be taken off the table merely because of fears of political opposition or the daunting complexity of the task. Serious study and consideration should be given to measures that could positively influence the legal, policy, and economic environment in which information technology is deployed so that our vulnerabilities can be minimized as efficiently and effectively as possible, without inhibiting technological innovation.